

PAI Partners

Whistleblowing procedure

Version	Release date	Description	Approved by:
V1	March 2021	Initial Procedure	Management Committee

Table of Contents

1. Scope	3
2. Whistleblowing process	4
2.1 Whistleblowing definition	4
2.2 Activities covered by whistleblowing protection	4
2.3 Reporting of facts	5
2.4 Confidentiality	5
2.5 Protection against retaliation	6
3. Processing of the alerts	7
3.1 Whistleblowing Referents	7
3.2 Processing of the alerts	7
3.3 Monitoring of reports	8
3.4 Processing of personal data	8
3.5 Distribution	8
3.6 Information	9
3.7 Review of the procedure	9
Appendices	10
1. Data protection	10
2. Subjects covered by whistleblowing procedure	11
3. Regulations	12

1. Scope

The **Whistleblowing procedure** is designed to provide uniform standards for the whistleblowing rules applicable to PAI Partners SAS (the “**Company**”), PAI Partners S.à r.l. and their affiliates (all together, the “**Group**”). The procedure will be applied by all entities within the Group, in addition to their local regulatory requirements.

This procedure comprises the internationally accepted whistleblowing principles without replacing the existing national laws. It supplements the national data protection laws. The relevant national law(s) will take precedence if it conflicts with this procedure, or it has stricter requirements than this procedure. The content of the procedure must be observed in the absence of corresponding national legislation. Each Group company is responsible for compliance with this procedure and its legal and regulatory obligations. In the event of conflicts between national legislation and this procedure, PAI will work with the relevant Group company to find a practical solution that meets the purposes of the procedure.

This process is subsidiary and does not intend to replace the standard internal communication channels established through the hierarchical structure of each Group company, such as the line manager of a staff member or in the event that the staff member does not wish to refer the matter to the line manager, the Compliance Department or the Human Resources department.

What is Whistleblowing?

To blow the whistle is to alert a third party that a person or entity has done, or is doing, something wrong. So, literally, “whistle-blowing” means that a party, in good faith, conveys or transmits a concern, allegation or information indicating that a prohibited practice is occurring or has occurred in the Group.

Staff members of PAI may bring to attention, in a confidential manner, any serious infringement of the general interest, breach of laws and regulations or internal procedures.

The Group makes it possible for any staff member to inform of any potential or actual breach of the legal and regulatory provisions, as well as internal procedures.

The procedure allows those who wish to do so to exercise their whistleblower rights and to benefit from the whistleblower protection provided by the relevant regulation (please refer to Appendix 1).

2. Whistleblowing process

2.1 Whistleblowing definition

A whistleblower (the “**Whistleblower**”) is any person falling into a category below:

- any staff member who is permanent or temporary employee e.g., full-time, part-time, secondees, interns or alternants;
- any suppliers (including its employees), freelancers, subcontractors;
- any third party related to the Group such as investors, business service providers etc.

The Whistleblower must act:

- in good faith, i.e., with the belief that the facts are true at the time they are reported;
- selflessly, i.e., the Whistleblower shall not intend to receive any compensation, benefits, or consideration, and does not act with the intention to harm another person.

Whistleblowers must have personally become aware of the facts reported. The reporting of facts of which an individual has not become personally aware, having been told by another person, or which stems from a suspicion or an unsubstantiated allegation, will be considered inadmissible.

The Whistleblower should not in any case try to conduct his/her own investigation.

2.2 Activities covered by whistleblowing protection

Whistleblower rights protect any person who decide to report a serious violation of the general interest of which he/she is personally aware.

The subject of the report may be any crime or offense, any serious and clear violation of rules and regulations, a law or an international treaty, or any serious threat or damage to the general interest.

To illustrate, the report may relate to any fact or conduct constituting a violation of the rules regarding:

- any violation of regulation and/or law (national or international);
- breach of professional and ethics rules;
- infringements of the rules for the protection of clients' interests;
- leakage of confidential information;
- inappropriate or unprofessional behavior towards employees, including sexual and moral harassment, discrimination;
- acts of fraud, embezzlement, and theft;
- acts of corruption;
- anti-competitive practices;
- violation of regulation or laws or internal procedures;
- acts of fraud, negligence, breach of trust or duty;

- violation of human rights;
- any damage to the health and / or safety of persons or the environment noticed within activities performed by the Group or, by the portfolio companies in which the managed Funds invest or, by suppliers;
- financial crimes (sanctions, embargoes, market abuse); and
- any issues that may harm reputation of the Group.

2.3 Reporting of facts

In accordance with the regulation, PAI Partners has implemented a dedicated whistleblowing channel (through an external secure platform) to receive and manage reports:

<https://paipartners.signalement.net>.

The examination and processing of the reports are carried out by the Company in complete confidentiality.

The report must be factual and should not be speculative. It should contain any relevant information or documents supporting the reported facts to allow a proper assessment of the nature and the extent of the concern. It should be as exhaustive, accurate, as detailed as possible.

The Whistleblower is invited to provide his/her contact details information (name, surname, contact details) for corresponding with the Referents, as defined in section 2. The Group undertakes to keep such information confidential (refer to section below).

By way of exception, an anonymous report may be processed, provided that the gravity of the concerns justified an investigation.

After having submitted a report, the system generates an automatic confirmation of receipt to the Whistleblower. This code allows for a confidential exchange with the Group's Referents in charge of the report.

Any whistleblowing report made, whether openly, confidentially, or anonymously, shall be promptly reported to the Group Risk Committee (" Risk Committee") but the name of the Whistleblower shall not be divulged. The Risk Committee will review the facts reported and, at its discretion, request for an internal or external expert to assist in the investigation.

If any member of the Risk Committee has a conflict of interest in any given case, then he/she should excuse himself/herself from the meeting.

2.4 Confidentiality

The Group guarantees the strict confidentiality of:

- the identity of the Whistleblower;
- the identity of the individuals referred to in the report;
- all information collected as part of the processing of the report.

The identity of the concerned staff member person will be kept confidential to the extent possible, given the legitimate needs of law and the investigation.

The Referents (refer section 2) or any internal teams or external advisors appointed (the **"Representatives"**) to assist on the investigation or any other person who have access to information pertaining to a whistleblowing report will take all necessary measures, including:

- Securely storing collected information in electronic or physical format.
- Ensuring anonymity of the Whistleblower.
- Limiting the number of individuals informed to strictly those who need to know.
- A transmission of any information to external advisors or authorities which must not identify the Whistleblower, unless the Whistleblower gives its prior consent.

External advisor(s) will sign a Confidentiality Agreement. It undertakes also not to use the data for the wrong purposes, to ensure its confidentiality, to comply with the limited data retention period and to proceed with the destruction or the return of the manual or computerized materials containing personal data when it ceases to provide its services.

The exchanges between the Referents (and/or his/her potential Representatives) and the Whistleblower should take place through the external secure platform.

2.5 Protection against retaliation

The Group protects any individual having notified facts constituting an offence or a crime in a selfless manner and acting in good faith, even if the reported facts should prove inaccurate, or no subsequent actions are undertaken, particularly:

- no individual may be excluded from a recruitment process or prevented from accessing an internship or a period of training within the Group; and
- no employee may be sanctioned, dismissed, or face any direct or indirect discriminatory measure, in particular in terms of remuneration, incentive or share distribution measures, training, reclassification, assignment, qualification, classification, professional promotion, transfer or contract renewal.

Any employee who considers that he/she has faced retaliation for having reported or provided evidence, may in good faith report such situation to the Referents or the Human Resources.

PAI Partners strongly encourages the Whistleblower to provide his/her details in order for the Group to fully protect him/her under this whistleblowing procedure.

Any misuse of the mechanism by false reports (notification of information known to be totally or partially inaccurate) or acting in bad faith makes the Whistleblower liable to the prosecution provided by law and, in accordance with the Internal Regulations, to disciplinary sanctions.

Any employee hindering or having hindered the submission of a report or having engaged in retaliation against a Whistleblower, may be subject to prosecution and may also face disciplinary sanctions, in accordance with the Internal Regulations.

3. Processing of the alerts

3.1 Whistleblowing Referents

The referent receives and analyzes the reports submitted.

The Referents are the Head of Compliance and the Legal Director unless there is a clear conflict of interest. In this case, the Management Committee will authorize and appoint an independent person to investigate.

The Risk Committee ensures the absence of conflict of interest by any member involved in an investigation and ensures the replacement of the Referent (and his/her Representative) where needed (i.e., absence, vacations, etc.).

PAI Partners S.à r.l. (Luxembourg), subsidiary of the Company, being authorized in Luxembourg as an Alternative Investment Fund Manager, is subject to the supervision of the Commission de Surveillance du Secteur Financier (the “**Luxembourg Regulator**”). Regarding this, any alert received from an employee of PAI Partners S.à r.l. or concerning PAI Partners S.à r.l. or relating to Luxembourg funds or SPVs, must be reported to the relevant conducting officers authorized by the Luxembourg Regulator.

3.2 Processing of the alerts

The decision to investigate Whistleblower’s claims taken by the Risk Committee is not an accusation and is to be treated as a neutral investigation.

In handling a report, the Referents may require the support of internal teams or external advisors.

The Referents and his/her Representatives shall derive their authority and access rights from the Risk Committee. They must be independent and unbiased.

The Group aims to handle the report as follows:

- Examination of the admissibility of the report will be carried out within fifteen (15) business days following receipt of the report. The Whistleblower shall be informed of the Risk Committee decision.
- If the report is admissible, an investigation will be carried out within three (3) months maximum. However, in exceptional circumstances, the timeframe of such investigation may be extended.
- If needed, a general update without specific details may be provided to the Whistleblower during the investigation phase.

- At the end of the investigation, the Referents and/or the Representatives will provide the Risk Committee with a report including:
 - o Recommendations (to close the investigation without any action, launch a disciplinary process, inform the authorities etc.);
 - o An action plan for remediation if needed;
 - o The possible disciplinary sanctions to be imposed on a Whistleblower in the event of a report made in bad faith.
- An information of the general outcome and closure report will be provided to the Whistleblower.

The Referents and his/her Representatives shall update on a regular basis the Management Committee and the Risk Committee if required.

3.3 Monitoring of reports

In order to be able to assess the effectiveness of the whistleblowing mechanism, the Referents may implement an annual statistical monitoring of the reception, processing and the subsequent actions taken with regard to each report.

Such annual statistical monitoring may indicate the number of reports received, closed files, reports having resulted or resulting in an investigation, as well as the number and the type of measures taken during and following the investigation (protective measures, disciplinary proceedings or legal actions, imposed sanctions, etc.).

3.4 Processing of personal data

The Referents, as the person responsible for processing, take all precautions needed to ensure the security and integrity of the collected data, both at the time of collection and processing of the data and at the time of communication for investigation purposes and recordkeeping after the case is closed.

In accordance with the internal procedure detailed in Appendix 1, the Whistleblower has rights regarding its personal data (right to access, correct its personal data, etc).

3.5 Distribution

The Group will notify its staff of their whistleblowing rights, including, for example, by means of a notice from the Management Committee or by addressing a notification.

3.6 Information

Requests for information regarding whistleblowing rights will not be considered as a report falling within the scope of the mechanism set forth in this procedure.

3.7 Review of the procedure

This procedure is approved by the Management Committee and will be reviewed at least every three (3) years and may be revised by the Compliance Department at any time beforehand on a proposal by any staff member or due to any change of the relevant regulations.

Appendices

1. Data protection

As part of the processing of a Whistleblower's report and in order to comply with the relevance and minimization principles, the Group only records the following data:

- identity, duties and contact details of the Whistleblower.
- identity, duties, and contact details of the individuals who are the subjects of a report.
- identity, duties, and contact details of the individuals involved in the receipt or processing of the report.
- facts reported.
- information collected as part of the verification of the reported facts.
- report of the verification operations.
- subsequent actions following the report.

The information provided as part of this report may contain highly sensitive personal data (such as for instance, personal data that reveals ethnic or racial origin, political opinions, religious or other convictions, or philosophical or trade union membership of an individual, genetic, biometrics or health data or data concerning sexual life or orientation of a person) or special categories of personal data (such as for instance, data related to offences, convictions and security measures concerning natural persons). The processing of such personal data is performed by the Group only if authorized by specific provisions of national law or in order to allow the Group to prepare and, where appropriate, to exercise and monitor legal action as or on behalf of a victim or a defendant.

The purpose of the collection and processing of such personal data is to determine the admissibility of the notifications, to verify the facts and take any remedial actions that may be required. Such actions therefore allow the Group to comply with its legal obligations and to protect its legitimate interests (by complying with the ethical principles of the Group).

Such personal data is only accessible to the Whistleblowing Referents, who are authorized persons to have access to them considering their duties, as well as to the external third party acting on behalf of the Group in charge of the management of the secured platform <https://paipartners.signalement.net>. The recipients of this personal data can be also each Group company if necessary, as well as the judicial authority, with the consent of the person.

Any transfer of this personal data outside the European Union is performed based on appropriate safeguards. The right of access, rectification, deletion, limitation and opposition to the processing of data may be exercised, within the legal and regulatory framework, by contacting the Whistleblowing Referent through the secure mailbox on the platform or the Data Protection Officer (DPO) at dataprotectionofficer@paipartners.com. The right to lodge a complaint before the competent data protection authority may also be exercised (in France, before the CNIL at <https://www.cnil.fr/fr/plaintes>).

Any individual who is the subject of a report cannot obtain information regarding the identity of the Whistleblower from the person in charge of its processing under any circumstances.



The Whistleblower or the individual that is the subject of a report may be assisted by a person of his/her choice working for the Group at any stage of the mechanism.

Any data relating to a report that is considered not to fall within the scope of the mechanism of this procedure will be deleted or archived after anonymization by the Group.

If no follow-up action is taken regarding a report, the Group will destroy all of the elements pertaining to the report allowing to identify the Whistleblower and the individuals that are the subject of the report. Such destruction will be carried out at the latest two (2) months after the closure of all of the operations of admissibility, investigations and verification of the report.

If there are disciplinary proceedings, legal actions, regulatory requirements following up or related to the report, the data relating to the report will be retained until the end of such proceedings or statute of limitations of appeal against the decision.

The Group has taken all necessary precautions in view of the risks presented by its processing in order to preserve the security of personal data and, in particular, at the time of their collection, during their transmission and storage, to prevent them from being deformed, damaged or that unauthorized third parties have access to it.

Prior to the implementation of this mechanism, a Data Privacy Impact Assessment (DPIA) has been performed by the Group, as required by the CNIL's Deliberation n°2018-327 dated 11 October 2018.

2. Subjects covered by whistleblowing procedure

- Conflict of Interest
- Fraud, embezzlement and theft
- Environment Protection
- Health and Security
- Discrimination and Harassment
- Regulatory, laws and internal procedures compliance
- Personal Transactions
- Data Privacy and Cybersecurity
- AML/KYC
- International sanctions and embargoes
- Tax Compliance and Transparency
- Corruption
- Financial Crimes
- Trade Secrets
- Market abuse

3. Regulations

Country	Regulation
France	Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernization of economic life (Loi Sapin 2)
Germany	Section 4d of the German Act establishing the Federal Financial Supervisory Authority (FinDAG) (Amendment in July 2016)
Italy	Loi No. 179/2017 - 29 December 2018, Loi No. 190/2012 "Anti-Corruption Law", Legislative Decree no. 231 of 8 June 2001
Luxembourg	CSSF Circular 18/698 of 23 August 2018: §160 and §260
Spain	Organic Law No. 3/2018 of 5 December 2018 on the Protection of Personal Data and the Guarantee of Digital Rights: Art. 24
Sweden	Act on Special Protection Against Victimization of Workers who Sound the Alarm on Serious Wrongdoings (2016:749)
United Kingdom	Public Interest Disclosure Act (1998), Employment Rights Act (1996)
United States	Whistleblower Protection Act (1989), Whistleblower Protection Enhancement Act of 2012, False Claims Act, Sarbanes-Oxley Act, Dodd-Frank, Occupational Safety and Health Act 1970, Defend Trade Secrets Act of 2016